المقدمة:

في ظل ما يشهده العالم من تزايد مستمر في الجرائم الإلكترونية وتطور أساليب اختراق الشبكات والأنظمة، أصبحت الحاجة ملحة إلى تطوير آليات استجابة قوية للحوادث الرقمية، مع وضع ضوابط دقيقة وفعالة لملاحقة الجنايات الإلكترونية. فالبيانات الرقمية باتت معرضة للاختراق بطرق معقدة، مما يفرض على المؤسسات امتلاك بنية تحكم إلكتروني داخلي متينة قادرة على مواجهة هذه التحديات.

تأتي دورة "إدارة عمليات البحث الجنائي" لتزويد المشاركين بمجموعة متكاملة من المهارات التقنية والإجرائية التي تمكنهم من إجراء التحقيقات في الجرائم والمخالفات الرقمية داخل المؤسسات أو خارجها. تشمل هذه الدورة تطبيق إجراءات متخصصة لاستخلاص الأدلة الرقمية من مختلف أنواع الأجهزة الإلكترونية مثل الحواسيب والهواتف المحمولة، وذلك وفقًا للمعايير العالمية التي تضمن الحفاظ على سلامة الأدلة الرقمية واعتماديتها أمام الجهات القانونية.

كما تتناول الدورة متطلبات عمل فرق الاستجابة للحوادث الأمنية (SOC وCSIRT)، حيث يتم تدريب المشاركين على كيفية أداء التحقيقات الرقمية بما يتوافق مع أفضل الممارسات والمعايير الدولية في هذا المجال.

الفئات المستهدفة:

- مختصو تكنولوجيا المعلومات الراغبون في تعزيز قدراتهم في التحقيقات الرقمية.
- فرق التحقيق في الاحتيال، مدققو الحسابات، وأعضاء فرق الاستجابة لحوادث أمن المعلومات (CSIRT).
- محللو مراكز العمليات الأمنية (SOC) في المؤسسات المعرّضة للمخاطر السيبرانية.
- أفراد الشرطة، القوات العسكرية، ضباط مراقبة السلوك، وأفراد الأمن العاملين في مجال التحقيقات الإلكترونية.
- المهتمون بتطوير معارفهم ومهاراتهم في مجال الطب الجنائي الرقمي والتحقيقات السيبرانية.

الأهداف التدريبية:

مع نهاية الدورة، سيكون المشاركون قادرين على:

- تطبيق منهجيات الطب الجنائي الرقمي ضمن بيئات العمل المختلفة.
- تصميم وتطبيق استراتيجيات فعالة لاستجابة الحوادث الرقمية والتحقيق الجنائي.
- تنفيذ تحقيقات رقمية متقدمة تشمل وسائل التواصل الاجتماعي، البرمجيات الخبيثة، والهجمات الفيروسية.
- إدارة مشاهد الجرائم الرقمية وضمان سلامة الأدلة الرقمية والحفاظ عليها دون تغيير.

- التحقيق في الأجهزة المحمولة ووسائط التخزين الرقمية التي قد تحتوي على بيانات جنائية.
- استخدام أدوات وتقنيات متخصصة في استخراج وتحليل الصور والبيانات الرقمية ذات الصلة.

الكفاءات المستهدفة:

- القدرة على إجراء تشريح جنائي رقمي مع إلمام بالمفاهيم القانونية المصاحبة.
- فهم القوانين والتشريعات المرتبطة بالجرائم الإلكترونية والتحقيقات الرقمية.
- التمكن من جمع الأدلة الرقمية ومعالجتها وحفظها بشكل قانوني وآمن.
- استخدام نظام اسم النطاق (DNS) كأداة مساعدة في التحقيقات الجنائية.
- تنفيذ تحقيقات متقدمة تشمل الجرائم الرقمية الداخلية والخارجية.
- توظيف تقنيات OSINT (المصادر المفتوحة) في جمع المعلومات والأدلة.

محتوى الدورة:

الوحدة الأولى: الجنائي الرقمي - الأسس والخلفية القانونية

- التعريف بمفهوم الطب الجنائي الرقمي وأهدافه ومجالات تطبيقه.
- استعراض تاريخ تطور الجرائم الرقمية وتحولاتها عبر الزمن.
- دراسة المصطلحات المستخدمة في التحقيقات الرقمية وتعريفاتها القانونية.
- التعرف على القوانين والأنظمة المتعلقة بالتحقيقات الجنائية الرقمية على المستوى المحلي والدولي.
- شرح المعايير الواجب اتباعها لقبول الأدلة الرقمية في المحاكم.
- تحليل أنواع المخاطر الرقمية التي قد تواجه المؤسسات.
- توضيح دور المستجيب الأول في الجرائم الرقمية والأدوات التي يحتاج إليها.
- التعرف على هيكلية عمل مركز العمليات الأمنية (SOC) وفريق الاستجابة لحوادث أمن المعلومات (CSIRT).
- تنظيم توزيع الأدوار والمسؤوليات بين الفرق الفنية والقانونية.
- تنفيذ خطة استجابة متكاملة لإدارة الحوادث الرقمية والتحقيقات المرتبطة بها.

الوحدة الثانية: جمع ومعالجة الأدلة الرقمية

- استخدام نظام DNS كأداة تحليل وتحقيق في الجرائم الرقمية.
- التعامل مع البنية التحتية الأمنية عند جمع الأدلة الرقمية.
- التحقيق في محتويات الهواتف المحمولة والتقنيات المتنقلة.
- استعراض الأدوات التقنية المتقدمة لاستخلاص الأدلة الرقمية وتحليلها.
- تجهيز الأدلة الرقمية بشكل منهجي لاستخدامها في التحقيقات والمحاكم.
- تطبيق البروتوكولات الأمنية عند التعامل مع الشبكات اللاسلكية والأدلة المحمولة.
- إعداد التقارير الاحترافية التي توثق نتائج التحقيق الرقمي وتدعم القضية.

الوحدة الثالثة: التحقيقات في الجرائم الرقمية الداخلية والخارجية

- تحديد الفروقات الجوهرية بين الجرائم الرقمية الداخلية والخارجية.
- استخدام أدوات OSINT في جمع المعلومات من المصادر العامة والعلنية.
- تحليل تأثير البرمجيات الخبيثة وبرامج الفدية على أنظمة المؤسسات.
- دراسة أساليب مكافحة الإرهاب الرقمي والجريمة السيبرانية.
- تطبيق استراتيجيات متقدمة لمكافحة التهديدات الإلكترونية.

الوحدة الرابعة: الاستجابة للحوادث الرقمية

- تصميم خطة شاملة للاستجابة لحوادث الأمن السيبراني.
- تنفيذ الأدوات اللازمة لرصد وتحديد الهجمات الرقمية.
- تعزيز التنسيق بين الفرق الأمنية والتقنية لضمان سرعة الاستجابة.
- تحليل ما بعد الحادث واستخلاص الدروس المستفادة من التجربة.

الوحدة الخامسة: التطبيقات العملية في التحقيق الجنائي الرقمي

- تنفيذ تحقيقات رقمية محاكاة لتطبيق النظريات المكتسبة.

- تحليل الأدلة المستخلصة باستخدام أدوات احترافية.
- تطبيق تقنيات استرجاع البيانات والصور من الأجهزة المصابة.
- تنفيذ خطوات تأمين الأدلة الرقمية وحمايتها من التعديل أو التلف.

الوحدة السادسة: إدارة عمليات البحث الجنائي

- تحديد الأهداف الأساسية لعمليات البحث الجنائي ودوافعها.
- التخطيط المسبق والمنهجي لعمليات البحث الجنائي.
- تنظيم فرق البحث وتوزيع المهام حسب المهارات والتخصصات.
- قيادة الفرق أثناء تنفيذ عمليات البحث وفق معايير السلامة والدقة.
- تجنب الأخطاء الشائعة وتحسين كفاءة الأداء في إدارة العمليات.

الوحدة السابعة: التحريات الجنائية

- تحديد مصادر جمع المعلومات الجنائية وكيفية الاستفادة منها.
- إدارة المصادر البشرية وتوظيفها في دعم التحقيق.
- استخدام آليات المراقبة الأمنية وأدواتها في جمع الأدلة.
- توظيف التكنولوجيا الحديثة لخدمة عملية التحقيق.
- إجراء مناقشات تفصيلية مع المشتبه بهم والمتهمين بأساليب قانونية وأخلاقية.